セキュリティログ要約レポート

要約

- ログには3つのイベントが記録されている。
- 192.168.1.25からのuserAのログオン失敗が15回記録されている。
- 192.168.1.100のadminユーザーによるログオン成功が1回記録されている。
- 192.168.1.30からのuserBのログオン失敗が7回記録されている。

リスク評価

- userAとuserBのログオン失敗が繰り返し発生しており、不正アクセスの試行の可能性が高い。
- 特にuserAの15回のログオン失敗は異常な挙動であり、セキュリティ上のリスクが高い。
-

adminユーザーによるログオン成功は1回のみであり、正当なアクセスである可能性が高いが、監視が必要。

対応策

1. **userAおよびuserBに関する対応**

-

ログオン失敗が繰り返し発生しているため、アカウントロックアウトポリシーを適用する。一定回数のログオン失敗後、アカウントをロックすることで不正アクセスを防ぐ。

-

ログオン失敗の原因を調査し、不正アクセスの可能性がある場合はアカウントのパスワードをリセットする。

2. **adminユーザーに関する対応**

-

adminユーザーのログオン成功は1回のみであり、正当なアクセスである可能性が高いが、監視を強化する。不審なアクティビティが検出された場合は、緊急対応を行う。

3. **セキュリティ強化策**
   - ログの監視を強化し、不審なアクティビティを早期に検知できるようにする。
-
ユーザーに対してセキュリティ意識向上のトレーニングを実施し、不正アクセスやフィッシング詐欺などに対する警戒心を高める。